WHAT IS CLAIMED IS:

1. In a computing device, a system comprising:

an interchangeable cryptographic module including at least one algorithm for converting unencrypted data into encrypted data and converting encrypted data into unencrypted data; and

file system level software that maintains files on a non-volatile storage including reading and writing file data to the files on the non-volatile storage, the file system level software configured to:

1) identify a file maintained on the non-volatile storage as an encrypted file;

2) receive a request to write presently unencrypted file data to the encrypted file, and in response:

a) to communicate with the installable software component including providing key data to convert the unencrypted file data into encrypted file data, and

b) to write the encrypted file data to the encrypted file on the non-volatile storage;

and

3) receive a request to read file data from the encrypted file, and in response:

a) to read the encrypted file on the non-volatile storage to obtain encrypted data

corresponding to the request,

b) to communicate with the installable software component including providing key data to convert the encrypted data into unencrypted data, and

c) to return the unencrypted data.

2. The system of claim 1 wherein the interchangeable cryptographic module includes a plurality of algorithms, and wherein the file system level software specifies a selected algorithm to use.

3. The system of claim 2 wherein the file system level software specifies which algorithm to use by calling a selected function of the interchangeable cryptographic module that corresponds to the selected algorithm.

4. The system of claim 3 wherein the file system level software indicates whether encryption or decryption is desired by passing data to the interchangeable cryptographic module when calling the selected function thereof.

5. The system of claim 1 wherein the interchangeable cryptographic module registers functions with the file system level software.

6. The system of claim 1 wherein the interchangeable cryptographic module and the file system level software comprise kernel mode components.

7. A computer-implemented method, comprising:

operably connecting an interchangeable cryptographic module to file system level software, the interchangeable cryptographic module including a plurality of selectable algorithms for converting unencrypted data into encrypted data and converting encrypted data into unencrypted data;

the file system level software:

1) receiving a request to read file data from an encrypted file;

2) obtaining key data that corresponds to a key to use and algorithm data corresponding to a selected algorithm of the plurality to use for data decryption;

3) reading encrypted file data corresponding to the requested data from the encrypted file; and

4) returning unencrypted file data corresponding to the request by communicating with the interchangeable cryptographic module to invoke the selected algorithm and decrypt the encrypted file

data into the unencrypted file data via the key.

8. The method of claim 7 wherein the file system level software obtains the algorithm data corresponding to a selected algorithm from information on the non-volatile storage associated with the encrypted file.

9. The method of claim 7 wherein the file system level software invokes the selected algorithm of the cryptographic module by calling a function corresponding to the algorithm with input buffer, output buffer, and key-related data.

10. A computer-readable medium having computer-executable instructions for performing the method of claim 7.

11. In a computer system, a method comprising:

receiving information at file system level software indicating that a file has encrypted file data stored in a non-volatile storage;

obtaining a key for decrypting the file data from key information maintained in association with the file on the same non-volatile storage as the encrypted file data; and

receiving a request to read encrypted file data of the encrypted file from the non-volatile storage, and in response,

reading the encrypted file data from the non-volatile storage, decrypting the encrypted file data into decrypted file data at the file system level software using the key, and returning the decrypted file data.

12. The method of claim 11 wherein the request is received from an application that is unaware that the file data is encrypted.

13. The method of claim 11 further comprising receiving a request to write presently unencrypted file data to the encrypted file on the non-volatile storage, and in response, encrypting the presently unencrypted file data into encrypted file data at the file system level software with an encryption key corresponding to the key for decrypting the file data, and writing the encrypted file data to the non-volatile storage.

14. The method of claim 11 wherein the file system level software includes a file system component and an encryption/decryption software component linked thereto that decrypts the encrypted file data into decrypted file data.

15. The method of claim 11 further comprising, registering functions of the encryption/decryption software

component with the file system component.

16. The method of claim 11 wherein the file system level software includes a file system component and an algorithm component separate therefrom that provides at least one algorithm for performing encryption and decryption operations.

17. The method of claim 11 wherein the file system level software includes a file system component and an encryption/decryption software component linked thereto that decrypts the encrypted file data into decrypted file data using an algorithm component separate therefrom that provides at least one encryption/decryption algorithm.

18. A computer-readable medium having computer-executable instructions for performing the method of claim 11.

19. A computer-implemented method, comprising:

operably connecting an interchangeable cryptographic module to file system level software, the interchangeable cryptographic module including a plurality of selectable algorithms for converting unencrypted data into encrypted data and converting encrypted data into unencrypted data;

the file system level software:

1) receiving a request to write presently unencrypted file data to an encrypted file;

2) obtaining key data that corresponds to a key to use and algorithm data corresponding to a selected algorithm of the plurality to use for data encryption;

3) communicating with the interchangeable cryptographic module to invoke the selected algorithm and encrypt the unencrypted file data into the encrypted file data via the key; and

4) writing the encrypted file data corresponding to the request to the encrypted file on the non-volatile storage.

20. The method of claim 19 wherein the file system level software further writes information identifying the selected algorithm to the non-volatile storage in association with the encrypted file.

21. The method of claim 20 wherein the file system writes information identifying the selected algorithm to the non-volatile storage in association with the encrypted file by writing data into part of the encrypted file such that the selected encryption algorithm can be later determined by

reading that part of the file.

22. The method of claim 19 wherein the file system level software invokes the selected algorithm of the cryptographic module by calling a function of the cryptographic module that corresponds to the selected algorithm.

23. In a computer system having a file system, a method of returning requested file data, comprising:

receiving at file system software a request to read file data of an encrypted file;

determining whether file data corresponding to the request is stored on a storage medium or has been decrypted to an access-controlled location; and

if the file data has been decrypted to the access-controlled location, returning the file data in decrypted form from the access-controlled location in response to the request; or

if the file data is stored on the storage medium, reading the file data corresponding to the request from the storage medium, calling an interchangeable cryptographic module to decrypt the file data into unencrypted file data, and returning the unencrypted file data in response to the request.

24. The method of claim 23 wherein calling an interchangeable cryptographic module comprises calling a function thereof based on an algorithm used to encrypt the data.